Subject	Date	Policy #
ITS Incident Response Policy	October 2021	ITS – 9.0
	Application	**Supersedes**
	ITS Security	
	Distribution	
	All Departments	
Recommended	**Approved**	
Preston D. Marx, VP Information Systems	James I. Marshall, Administrator - CEO	

1.0 Purpose

This policy defines the standards and procedures for business continuity during and after an interruption in normal business workflow. The policy does not attempt to specifically filter ITS response by severity or type of interruption or disaster. The intent is to provide general direction and protocol to the ITS staff and UBH employees in the event of an incident..

2.0 Scope

The policy applies generally to all areas of the organization acknowledging that the true scope of the plan will be determined by the size and duration of the interruption or disaster. This policy is meant to work in conjunction with other organizational and departmental level continuity plans and should not be given precedence over established plans.

3.0 Policy

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
- Fraud – Inaccurate information within databases, logs, files or paper records.

EXHIBIT 9

Reporting an Incident

The Security Officer should be notified immediately of any suspected or real security incidents involving sensitive data which includes: PHI, confidential personal files, intellectual property, or cardholder data:

Contact the ITS Service Desk to report any suspected or actual incidents. Their phone number should be well known to all employees and should reach someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Security Officer about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by Public Relations.

Document any information you know while waiting for the Security Officer to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner. (PCI Requirement 12.10.1)

Responding to an Incident

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

1. **Identification** - have tools in place to identify and alert when an incident is suspected. Staff must be trained to identify common signs of incidents.
2. **Severity Classification** - Assign the incident a threat level (Critical, High, Needs Attention, Warning). Report all critical or high incidents to the Security Officer immediately then proceed to the next step.
3. **Containment** - do what is necessary to patch the active threat and keep it from spreading or expanding. This might include isolation of workstation(s), disabling of user accounts, disconnecting all or parts of the network. Patient safety must be considered when implementing containment measures.
4. **Eradication & Recovery** - Use tools available to eliminate the threat. If not possible, then determine how containment measures can be left in place to isolate the threat. Create detailed notes on steps taken that can be shared with the leadership team.
5. **Root Cause Analysis and Lessons Learned**
   Not more than one week following the incident, members of the HIPAA Audit Committee and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the Incident Response Plan. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.